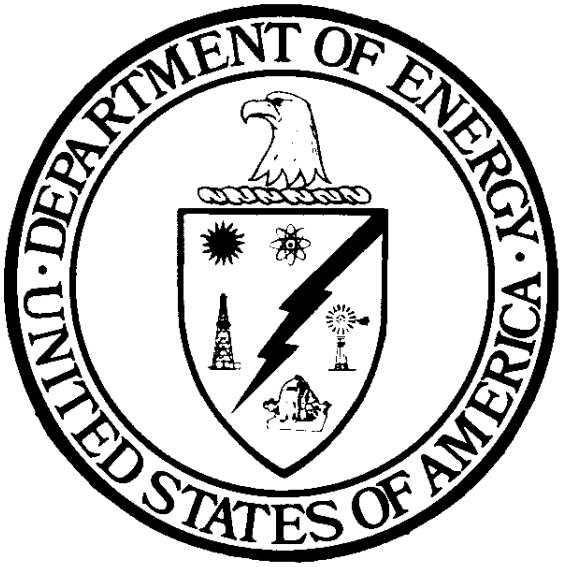
GUIDELINE FOR PREPARATION OF ACCEPTABLE USE AGREEMENTS FOR USERS OF COMPUTATIONAL RESOURCES



December 1995

U.S. Department of Energy
Assistant Secretary for Human Resources and Administration
Deputy Assistant Secretary for Information Management
Office of Information Management

GUIDELINE FOR PREPARATION OF ACCEPTABLE USE AGREEMENTS FOR USERS OF COMPUTATIONAL RESOURCES

TABLE OF CONTENTS

U.S. DEPARTMENT OF ENERGY

GUIDELINE FOR PREPARATION OF ACCEPTABLE USE AGREEMENTS FOR USERS OF COMPUTATIONAL RESOURCES

December, 1995

BACKGROUND

The development of this guideline grew from the collective efforts of a number of individuals from Department of Energy sites who attended an invitational symposium hosted by Lawrence Livermore National Laboratory (LLNL) in April 1995. In attendance were personnel with various areas of expertise, including: the Computer Security Programs (classified and unclassified); Legal; Law Enforcement; Education, Training and Awareness; and, Technical Engineering.

SUMMARY OF LLNL SYMPOSIUM ON COMPUTER USE AND GRAPHICS ON THE INTERNET

REASON FOR CONVENING THIS GROUP

The DOE suffered tremendous embarrassment due to an incident where considerable pornographic material was discovered on Federal computer systems. The Inspector General's office at Oakland Operations Office requested something be done about computer misuse, and suggested several ways they thought the issue could be addressed through a combination of technology and administrative procedures. The Information Management Division of the Oakland Operations Office requested that Lawrence Livermore National Laboratory convene a diverse group of technical, legal, and computer security program people to address the issue. This one and a half day symposium was the result of that request.

GOAL: "What is acceptable use"?

ISSUE RAISED:

To determine what an "acceptable use" baseline should be for DOE/DOE contractor site computational resources, we have to understand the variables (such as state statutes) which can affect how an organization does business.

WHAT WE LEARNED:

- Site representatives believe there is a need for a user agreement: (1) describing acceptable principles for the use of Federal computing resources; (2) stating the user gives consent to have these resources monitored; and, (3) the user understands their individual responsibilities as stated in the agreement.
- There are various statutes, both Federal and state, which must be considered when establishing acceptable principles for users of Federal computing resources.
- The cost of monitoring computer resource use makes it impractical to monitor full time.
- "WFA" (waste, fraud, and abuse) audits of computer systems serves best as a deterrent of system misuse.
- When cases of improper use of Federal computing resources are successfully processed, the consequences should be consistent. For this to take place, management must support the "punishment levels" established for the offense. However, it is realized there is always the possibility of extenuating circumstances, therefore each case has to be adjudicated individually.

- Managers must "manage" their employees in a fashion that is consistent site-wide and which supports the acceptable principles.
- Management's role -- "Follow Me!". Management has a role before, during, and after training, which is to be the leader in demonstrating accepted principles.
- Variations in "accepted principles" will appear at different sites due to differences in computing environments, mission of the site, and differences in management perspectives.
- A group synergy emerged during this symposium. We learned many sites are working in parallel, but not in collaboration. Thus, this symposium was very beneficial in that participants have identified "partners". We will benefit by networking and leveraging the group expertise.
- Issues raised during the discussion of "detection" (i.e., monitoring) related to privacy considerations, costs, and kinds of intrusions to be detected.
- We learned the difference between training and education: Training is done to create new behavior; Education creates awareness.

<u>WHERE DO WE GO FROM HERE?</u>

1. OAK and HQ will prepare a "white paper" on accepted principles, to be circulated to symposium attendees for comment. [*Sample "accepted use" policy statements were provided by representatives from the Albuquerque Operations Office, Pacific Northwest Laboratory, Lawrence Livermore National Laboratory, and the Los Alamos National Laboratory; Argonne National Laboratory provided a copy of their computer security policy.*]
2. After receiving comments on the "white paper" from symposium attendees, Headquarters and Oakland Operations Office will prepare a "white paper" on acceptable use for distribution to the group for discussion at the DOE CSG Training Conference on Monday afternoon, following Session C which ends about 3 p.m. This will be the second meeting of the Computer Use and Education Advisory Group.
3. Following the conference, HQ will finalize a draft on acceptable use for Mr. Hall's review.
4. Have document reviewed by Headquarters Office of General Counsel and Human Resources and Administration Office of Personnel Policy prior to finalizing for distribution.
5. Issue guideline.

ACKNOWLEDGMENTS

The DOE Office of Information Management thanks the following people who assisted in one or more ways with the development of this Guideline:

Computer Security Program Related Responsibilities
Phil Sibert, DOE HQ, CSPM
Chris Skowronski, DOE HQ, CDSI
Nancy Adair, OAK, CPPC
Charlene Douglas, LANL, CPPM/CSSM
Ted Combs, Allied Signal/KC, CPPM/CSSM
J. D. Fluckiger, PNL, CPPM
Carol Oliphant, Pantex, CPPM
Mark Rosenberg, LBL, CPPM
Jean Troyer, ANL, CPPM
D. Craig Jones, SNLA, CPPM/CSSM
Dave Grubb, LLNL, CPPM/CSSM
Steve Mick, LLNL
Frank Swift, LLNL
Joe Brandt, LLNL
Louise Beite, LLNL

Legal Staff or Law Enforcement
Paul Lewis, HQ, OGC
Rich Burta, OAK, OIG
Christine Gray Chandler, LANL, legal counsel
Max Creamer, LLNL, legal counsel
Gary Robinson, LLNL, protective forces

Technical Representatives
Chuck Athey, LLNL
Delmer Harris, Allied Signal/KC
Judy Lim, SNLA
Frank Maestas, LANL
Connie Soto, LLNL
Gregory Neal Thomas, Pantex
Cullen Tollbom, PNL

Education, Training, and Awareness
Tom Walsh, SAIC support to AIb.

Personnel Representative
Donald Dickerson, HQ, Office of Personnel

APPLICABILITY

This guideline may be applied to users of any Federal computer system operated by or on behalf of the Department of Energy.

REASONS FOR "RULES OF BEHAVIOR"or "USER PRINCIPLES"

Today's information system (IS) users are far more comfortable with using ISs than they were just 10 years ago. This is no doubt the result of the rapid proliferation of desktop computers and networking.

Given this increased confidence in IS users, national regulations and guidance are beginning to recognize that today's IS users must also be an intregal part of protecting Federal IS and the information that they store, process and/or transmit.

PUBLIC LAW 100-235, "COMPUTER SECURITY ACT OF 1987"

All Federal IS are covered by Public Law 100-235, "The Computer Security Act of 1987." The key Federal regulation implementing Public Law 100-235 is Office of Management and Budget (OMB) Circular No. A-130, Appendix III, "Security of Federal Automated Information."

OMB CIRCULAR No. A-130, APPENDIX III, "SECURITY OF FEDERAL AUTOMATED INFORMATION"

Below are excerpts from section 3 of Appendix III, highlighting the new requirements for "rules of behavior:" [NOTE: at this writing, these new requirements are in draft; however, the comment period closed in May 1995 and OMB expects to issue the final version of Appendix III with only minor changes, by the end of calendar year 1995.]

1. Purpose

This Appendix establishes a minimum set of controls to be included in Federal automated information security programs; assigns Federal agency responsibilities for the security of automated information; and links agency automated information security programs and agency management control systems established in accordance with OMB Circular No. A-123.

***At a minimum, agency programs should include the following controls in their general support systems and major applications**:*

*a. Controls for **General Support Systems**.*

1) *Assign Responsibility for Security.*
2) *System Security Plan. Plan for the security of each general support system...*
   Security plans should include:
   a) ***Rules of the System**. Establish a set of **rules of behavior** concerning use of, security in, and the acceptable level of risk for the system. The rules should be based on the needs of the various users of the system. The security required by the rules should be only as stringent as necessary to provide adequate security for information in the system. Such rules should clearly delineate responsibilities and expected behavior of all individuals with access to the system. They should also include appropriate limits on interconnections to other systems and should define service provision and restoration priorities. Finally, **they should be clear about the consequences of behavior not consistent with the rules.***
   b) ***Awareness and Training.***
   c) ***Personnel Controls**.*
   d) ***Incident Response Capability.***
   e) ***Continuity of Support**.*
   f) ***Technical Security.***
   g) ***System Interconnection.***

3) *Review of Security Controls.*
4) *Authorize Processing.*

*b. Controls for **Major Applications.***

1) *Assign Responsibility for Security.*
2) *Application Security Plan. Plan for the adequate security of each major application...*
   Application security plans should include:
   a) ***Application Rules**. Establish a set of **rules concerning use of and behavior within** the application. The rules should be as stringent as necessary to provide adequate security for the application and the information in it. Such rules should clearly delineate responsibilities and expected behavior of all individuals with access to the application. In addition, the **rules should be clear about the consequences of behavior not consistent with the rules.***
   b) ***Specialized Awareness and Training.***
   c) ***Personnel Security**.*
   d) ***Contingency Planning.***
   e) ***Technical Controls**.*
   f) ***Information Sharing**.*
   g) ***Public Access Controls.***

3) *Review of Application Controls.*
4) *Authorize Processing.*

SUGGESTED METHODS FOR IMPLEMENTING THIS GUIDELINE

The table below identifies suggested methods for implementing the template documents contained in this guideline: "**Computational Resources Users' Responsibilities (CRUR)**" and, "**[Site] Computer Use & Security Agreement (CUSA).**"

IMPLEMENTATION METHOD	CRUR	CUSA
Initial briefing or orientation of new employee	✗	✗
Re-orientation briefing when employee transfers	✗	✗
Orientation for employees on detail assignments	✗	✗
Annual employee performance evaluation	✗	
As part of **"Computer Security Day"** activities	✗	
As part of computer security awareness activities	✗	
As part of training (such as when an employee is connected to a LAN the first time, or when external network privileges are provided)	✗	✗
Annual security briefings	✗	

TEMPLATE DOCUMENTS

To assist sites in meeting the requirement for establishing rules of behavior, the Office of Information Management has developed two "template" documents. These documents make up the remainder of this Guideline. The template documents are titled:

"**Computational Resources Users' Responsibilities**" and,
"**[Site] Computer Use & Security Agreement**"

Each document is presented in a manner to allow your site to adopt it as is. These documents may also be modified to reflect your site's unique requirements.

IMPLEMENTATION NOTES

1.) Prior to implementation of the **"Computer Use and Security Agreement,"** or any variation thereof, be sure to confer with the union(s) representing employees at your site.

2.) These documents have been reviewed by the Department of Energy Office of General Counsel whose input has been included.

U. S. DEPARTMENT OF ENERGY

COMPUTATIONAL RESOURCES USERS' RESPONSIBILITIES

PRINCIPLES & RESPONSIBILITIES

Personnel who use any Federal computing resource (e.g., PDAs, notebooks/laptops, desktop PCs/Macs, workstations, other computers, data communication devices, and associated software and networks) at this site to process, store, or transmit data and information shall first read and familiarize themselves with the principles and responsibilities discussed below and sign the attached **COMPUTER USE & SECURITY AGREEMENT**, a signed copy of which will be retained by the user, and the original by the site.

FOR OFFICIAL APPROVED USE ONLY

Site computing resources are government property funded by the Department of Energy for the purpose of supporting the various programmatic and scientific research efforts needed to accomplish the Department's missions. As such, these resources are to be used only for official government business. Users should remember that when they use their organization's computing resources, they are acting in their employment capacity on behalf of their employer and the Department of Energy.

Electronic mail sent via site networks, for example, ordinarily bears site-specific identifiers in the address (*e.g.*, name@**hq.doe.gov** or name@**llnl.gov**). It therefore reflects on the Department of Energy and the site, indicating to all who read the message that it was composed on government equipment at a Federally funded site.

For these reasons, regardless of disclaimers, when you use site e-mail resources you are representing your site and the Department of Energy, and you must act accordingly. Because the e-mail that you send and receive through the site's computational resources is official business by definition, there ordinarily would be no legitimate reason to use anonymous remailers or personally owned copies of encryption software for the transmission of your messages. Unless approved by management, any activity outside the scope of your employment, or any activity which could embarrass the organization must be avoided.

MONITORING, RECORDING & AUDITING OF FEDERAL COMPUTING RESOURCES

Because these computational resources are government property, their use may be subject to monitoring, recording, and audits to insure the systems and networks are functioning properly, to protect against unauthorized access or use, and to ensure the confidentiality and integrity of data and information resident on the systems and networks. In addition, DOE or the Federal government may access any user's Federally provided computer system or data communications and disclose information obtained through such auditing to appropriate third parties, including law enforcement authorities. Users have **NO EXPECTATION OF PRIVACY** when using a site's Federal computing resources or public switched networks (*e.g.*, Internet, FTS-2000). Use of site Federal computing resources and network connections constitutes **EXPRESS CONSENT** by the user to monitoring, recording, and auditing for purposes identified above.

ENCRYPTION OF UNCLASSIFIED DATA AND INFORMATION

Unclassified data and information may be encrypted only with prior authorization of your supervisor and subject to such conditions and guidelines as may be established at your site. Whenever encryption is used, your supervisor must be provided the decryption key to ensure that encrypted information on Department of Energy systems will be available in the event the user is no longer available to decrypt the information.

MANAGER/SUPERVISOR RESPONSIBILITIES

All management and supervisory personnel must be aware of, and be leaders in applying these principles and carrying out these responsibilities. Supervisors are responsible for implementing these principles in their organization and will be accountable for ensuring that users are aware of, and acknowledge their responsibilities,

PRIVILEGED USERS' RESPONSIBILITIES

Privileged users are those having "super-user," "root," or equivalent access to a system (*e.g.*, system administrators or computer operators) which gives them near or complete control of the operating system of the machine or the IS. Because they can set up and administer user accounts and passwords, and because they generally have greater powers of access and use of computational resources than regular users, they have correspondingly greater responsibilities to avoid and prevent improper access to, and misuse of computational resources under their control, as well as to ensure the security and integrity of data and information contained in such computational resources.

Examples of Privileged Users include:

Users having access to change control parameters (routing tables, path priorities, addresses, *etc.*) on routers, multiplexors, and other key IS equipment.

Users who have been given the power to control and change other users' access to data or program files (*e.g.*, applications software administrators, administrators of specialty file systems, database managers).

Users who have been given special access for troubleshooting of IS/security monitoring functions (*e.g.*, those using IS analyzers, management tools).

VIOLATIONS

Acceptance of, and adherence to, these principles and responsibilities regarding appropriate use by all users of Federal computational resources is very important. Irresponsible conduct resulting in violations of these principles and site policy may lead to loss of system privileges and/or disciplinary action, up to and including termination of employment, as well as criminal penalties.

[SITE]

COMPUTER USE & SECURITY AGREEMENT

I have read and understand the **COMPUTATIONAL RESOURCES USERS' RESPONSIBILITIES** to which this **COMPUTER USE & SECURITY AGREEMENT** is attached. I agree that users of site computers, networks and information systems (IS) are an integral part of the overall Department of Energy computer security program (unclassified and classified). I also understand that this grant of access to the Department of Energy's computing resources indicates a level of trust bestowed upon me by my management and the Department of Energy. I agree that I am responsible for my actions, and I am aware of and acknowledge the following principles:

ACCEPTED USER PRINCIPLES

At a minimum, I am responsible for abiding by these principles:

- ☐ Ensuring that Federal computing resources are used only for official government business. Any other use must be approved in writing by my line manager.
- ☐ Knowing who my site computer security personnel are and how they can be contacted.
- ☐ Knowing the level of sensitivity of the information processed on my Federal computing resource (*e.g.*, non-sensitive unclassified, sensitive unclassified, or classified).
- ☐ Ensuring that all software I use is being used in compliance with applicable licensing agreements **and** has been authorized for use by my line manager.
- ☐ Protecting the information I am processing from access by, or disclosure to, unauthorized personnel.
- ☐ Immediately reporting all security incidents and potential threats and vulnerabilities involving Federal computing resources to the designated computer security personnel.
- ☐ Protecting my authenticators, such as passwords or smartcards.
- ☐ Reporting any compromise or suspected compromise of a password to the designated computer security personnel.
- ☐ Accessing only systems, networks, data, control information, and software for which I am authorized.
- ☐ Ensuring that system media and system output is marked according to site/system requirements and is properly controlled and stored.
- ☐ Knowing and ensuring required system storage sanitization procedures are carried out before relinquishing the system for service, or releasing it for any other reason except an audit, investigative action, or court order.
- ☐ Informing management when access to a particular Federal computing resource is no longer required, such as when I complete a project, transfer to another position, retire, resign from employment, *etc.*

- ☐ Avoiding the introduction of malicious code (*e.g.*, viruses, worms, trojan horses) into any computing resource.
- ☐ Preventing physical damage to the system.
- ☐ Obtaining management approval and notifying other appropriate personnel (*e.g.*, property management, inventory control, computer security) before relocating any Federal computing resources.

In the event that I am a **Privileged User**, I am also responsible for these additional principles:

- ☐ Protecting the root or superuser password at the highest level of data it secures and not sharing the password and /or account.
- ☐ All superuser or root actions under my account.
- ☐ Reporting any and all information system/network security-related incidents to the designated personnel.
- ☐ Using special access or privileges granted only to perform authorized tasks and functions.
- ☐ Using a non-privileged user account for everyday work not associated with the tasks of a superuser or system administrator.

To be completed by the user:

I, _____, have read the **COMPUTATIONAL RESOURCES USERS' RESPONSIBILITIES**
(print full name)
and understand my responsibilities as a user of Federal computing resources.

Signed:_____ Date:_____

To be completed by your supervisor of record:

I, _____, certify that _____ has been provided
(print full name)
computer security orientation, understands the responsibilities associated with using Federal computing resources, and has had all questions satisfactorily answered.

Signed:_____ Date: _____

To be completed by the designated site or cognizant computer security official:

I, _____, certify that the above named employee has been provided computer
(print full name)
security orientation.

Signed:_____ Date: _____